LA-UR-96-2365

Title: **Effective Vulnerability Assessment of Tamper-Indicating Seals**

Author(s): R.G. Johnston

Submitted to:

LAUR #96-2365

Effective Vulnerability Assessment of Tamper-Indicating Seals

R.G. Johnston

ABSTRACT: Security seals are widely used to detect tampering or unauthorized entry. In the author's view, existing standards for vulnerability assessment of security seals are incomplete. This paper discusses the critical attributes of effective vulnerability assessment. These include: a clear understanding of what seal vulnerability assessment is and why it is undertaken, use of appropriate assessment personnel, assessment at the earliest possible stage of seal development, analysis conducted with the proper emphasis and context, rejection of findings of zero vulnerabilities, avoidance of the term "tamper-proof", characterization of the degree of defeat, and thorough reporting of findings.

KEYWORDS: security seals, tamper-indicating seals, tamper-indicating devices, tamper-evident devices, tamper detection, tags, antipilferage

Introduction

Tamper-indicating devices, also called security seals, are widely used in industry and government [1-7]. Seals are not intended to stop unauthorized access. Rather, they are meant to leave unambiguous, non-erasable evidence of entry or tampering. Applications include access control, records integrity, inventory, shipping integrity, theft prevention/detection, hazardous materials accountability, nuclear nonproliferation, national defense, law enforcement, customs, counter-terrorism, counter-espionage, protecting instrument calibration and surveillance/monitoring equipment, testing for illegal drug use, and protecting consumer products [1-7]. Seals take a variety of forms [3-6]. Examples include frangible films or pressure sensitive adhesive tapes, crimped cables or other (supposedly) irreversible mechanical assemblies, security containers or enclosures that give evidence of being opened, devices or materials that are intended to display irreversible damage or changes when manipulated, and electronic systems that continuously monitor for changes such as a break in an electrical cable or fiber optic bundle.

As with any security device or security program, vulnerability assessments are useful for identifying seal problems and weaknesses. Existing security seal standards [5, 8-11] briefly discuss seal testing and vulnerability assessment. These standards, however, are far from comprehensive and, in the view of this author, fail to consider a number of issues critical to effective vulnerability assessment. The purpose of this paper is to discuss the attributes of effective vulnerability assessment, and to present ideas that might be relevant for future standards, as well as for increasing the efficacy of seal security testing.

The ideas contained in this paper are presented only as the personal views of the author. These views, however, form the underlying philosophy which he uses (as Team Leader) to direct the Seals Vulnerability Assessment Team at Los Alamos National Laboratory (LANL). This team has conducted vulnerability assessments on 92 different seal designs, both commercial and government. We have devised and demonstrated 129 successful attacks on the 92 seals, at least one successful attack per seal. Some of this work is discussed in references 12-14.

Existing Standards

ASTM Standard F1158-88, “Standard Guide for Inspection and Evaluation of Tampering of Security Seals,” is a one page standard concerned with both inspection and evaluation of security seals [8]. The standard indicates that it is not comprehensive, partially because certain types of seals (e.g., label seals) are not considered. Also, the standard "allows that any particular method of attempted defeat can be employed to defeat a seal, and concentrates not on the effectiveness of the seal to resist that attack, but rather on the nature of the individual seal to inhibit reapplication." The standard then offers suggestions for how to inspect various categories of seals to detect tampering. The types of seals that are considered include cable, wire, strap, cinch, bolt, rod, and padlock seals.

ASTM Standard F1157-90, “Standard Practice for Classifying the Relative Performance of the Physical Properties of Security Seals,” is largely concerned with strength of materials testing on security seals [9].
The United States Nuclear Regulatory Commission's January 1996 draft regulatory guide, "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material," specifies a number of required seal properties [5]. It has little to say, however, about vulnerability assessment.

U.S. Government Federal Specification FF-S-2738, “Federal Specification for Seals, Antipilferage,” indicates the minimum times that various seal types must withstand tampering [10]. Testing is to be done by U.S. Government approved laboratories. The specification, and its referenced documents, offer minimal guidance on how these tests should be conducted or on vulnerability assessment in general.

The British Standard BS 7480:1992, “Specifications for Security seals,” also establishes the length of time that various seal types must withstand tampering [11]. In Appendix A, it describes required physical tests and security tests. The latter are discussed in less than 1 page. The security tests involve attempts to "open and reclose the seal, using a variety of readily available and/or easily fabricated portable tools, such that interference with the container and the seal cannot readily be identified." According to the standard, acceptable tools that can be used to defeat a seal during the security tests include hand tools, specialty probes or wires, portable heating and cooling devices, and portable power tools. Acceptable attacks include attempting to pull the seal apart with force such that there is no apparent evidence of damage, manipulating the interior (e.g., picking)

to open the seal undamaged, thermal attacks, and disassembly of the seal followed by attempts to "replace, repair, or mask the damaged section(s) of the seal to disguise effectively the site of the attack when the seal is reinstated."

Suggestions for Effective Vulnerability Assessments

Seal Attacks and Defeats

For the discussion here, the term "attack" shall refer to an attempt to avoid detection while gaining entry through a seal to whatever the seal is protecting. A successful attack (one that is not detected) is also referred to as a "defeat".

Defeating a seal consists of opening the seal without any detected damage or evidence of entry; or opening the seal and repairing any damage and/or erasing detectable evidence of entry; or replacing the entire seal with a counterfeit that will be confused with the original; or replacing relevant parts with counterfeits. This general description of possible defeats is somewhat broader than that offered by ASTM Standard F1158-88 [8] or British Standard BS 7480:1992 [11].

The Purposes of Vulnerability Assessments

A comprehensive vulnerability assessment should involve more than simply trying to "certify" a particular seal. Goals should include the following:

1. Determine the effectiveness of the seal;
2. Identify its strengths, weaknesses, and vulnerability to attack;
3. Establish the appropriateness of the seal for a given application;
4. Attempt to find counter-measures for any identified vulnerabilities;
5. Suggest practical, often application-dependent, methods of improving the security of the seal, either by modifying the seal itself or by improving the installation, removal, or inspection procedures;
6. Improve the overall reliability of the seal and users' confidence in it.

Vulnerability Assessments Early in the Design Process

If possible, preliminary vulnerability assessments should be conducted at the early stages of the development of a new seal, while it is still relatively easy to make changes. Changes in a finished product are often difficult and costly.

Our experience at LANL suggests that an iterative approach is very productive. Suggestions for modifications to the preliminary design are offered by the vulnerability assessment team. If and when those changes are incorporated into the design, the modified seal design is then reanalyzed by the vulnerability assessment team. Multiple iterations of this process may be useful before a seal design is finalized.

Tools

Based on our experience at LANL, the tools listed under the British Standard are but a subset of the tools that are useful for defeating seals. It is probably unrealistic to expect that adversaries will or must limit themselves to hand tools, specialty probes or wires, portable heating and cooling devices, and portable power tools.

Personnel

Vulnerability assessments should be undertaken by personnel who are experienced in defeating security products. This idea is similar to that contained in the British Standard, which calls for tests to be conducted by "a technician experienced in the attempted compromise of physical security products" [11]. Our experience at LANL, however, suggests that seal testing should not be limited to technicians. More formally trained personnel are often of considerable value in devising and supervising seal attacks, even if technicians are often more skilled at executing them.

It is extremely important that assessors be external and independent. In-house vulnerability assessments may have some value, but they should not be viewed as acceptable substitutes for independent, external assessment. Assessments performed by the developer of a seal are usually of little value. A developer is unlikely to discover new vulnerabilities that were not envisioned during the design process.

It is also crucial that assessment personnel be psychologically predisposed to finding vulnerabilities. Assessors who are excessively beholden to the sponsor of the assessment, or who are reluctant--either consciously or unconsciously--to identify vulnerabilities are unlikely to

provide useful assessments. While it is difficult to measure psychological factors, assessors with a history of aggressively finding seal vulnerabilities are likely to have the appropriate attitude. Assessors with a history of failing to find significant vulnerabilities may not.
In general, finding vulnerabilities in security devices is best done by clever, innovative, and resourceful individuals. It is probably a mistake to assume that adversaries who might attempt to defeat a given security device do not have these attributes, or at least access to people who do. This is particularly true when adversaries may be highly motivated to defeat seals by personal financial gain or strong ideological, emotional, or fanatical views.

Context

To the extent practical, a seal vulnerability assessment should be done in the context of the relevant seal applications, purposes, environment, economics, personnel, training, adversaries, and defeat consequences. Protocols for seal procurement, storage, transport, installation, inspection, removal, and disposal should also be considered. Assessing the vulnerability of a seal in isolation of these factors limits the usefulness of the findings.

Emphasis

Vulnerability assessments should emphasize the simplest attacks and the weakest links in the chain of security. Complex, high-technology attacks are appropriate only after the low technology attacks have been thoroughly explored.

Physical Testing

In our experience at LANL, seal developers, manufacturers, and users sometimes fail to understand the difference between physical testing and security testing. Materials and strength testing may indeed be important for any given seal, and may be crucial components of vulnerability assessment. Physical testing alone, however, is not a substitute for vulnerability assessment.

Tamper-Proof Seals

No vulnerability assessment (nor seal developer, manufacturer, or user) should make the claim that a particular seal is “tamper-proof”. That assertion is ultimately unprovable, and probably a theoretical impossibility. Complete and total confidence in any security product, regardless of the findings of a particular vulnerability assessment, is probably ill-advised.

Findings of Zero Vulnerabilities

Our experience to date at LANL suggests that all seals have vulnerabilities. A vulnerability assessment should be suspect if it returns a finding of no vulnerabilities for a given seal, or if it offers no significant recommendations for improving the seal or the use protocol. Another vulnerability assessment--from different independent evaluators--should then be sought.

Reporting Findings

A comprehensive vulnerability assessment report should consist of the following 5 items:

1. A detailed description of the successful attacks. For each attack the following information should be provided:
   - Is the attack theoretical, partially demonstrated, fully demonstrated but not perfected, or practiced to perfection?
   - What are the cost, time, and effort to devise and demonstrate the attack?
   - What time is required on-site to do the attack?
   - How much time is required for the attack to become activated, which may differ from the time to do the attack? (It may, for example, take some time for the epoxy used in a particular attack to fully cure.)
   - What time is required for off-site preparation? (The British Standard permits off-site, pre-test preparation, but does not apply time constraints [11].)
   - What personnel, skills, technical sophistication, and costs are necessary to complete the attack?
   - How many times and for how long must the adversary have on-site access to the seal?
   - What is the size, weight, cost, and nature of the tools and materials that must be brought on-site for the attack?
   - What is the level of defeat? (See the next section.)
   - Is inside information necessary for the attack, or just what is publicly available?

2. Sample(s) of the defeated seal should be provided if practical and appropriate.

3. The report should include a discussion of possible counter-measures.

4. Samples of the seal employing the counter-measure(s) should be provided, if practical.

5. The report should include a statistical summary of the assessment that is purged of vulnerability and attack details, but that contains information on the identity of the persons/organization doing the vulnerability assessment, the level of effort for the vulnerability assessment, the number of attacks, time to develop them, time to execute them, type of defeats, number of possible counter-measures and their general nature. A seal developer, manufacturer, or user who claims that a particular seal has undergone vulnerability assessment should make this summary available to anyone to whom that claim is being made. An example of such a summary can be found in reference 13.

Categorizing Defeats: The LANL Defeat Categorization Scheme

It is important to classify the thoroughness of a seal defeat. In the author's view, it is overly simplistic to simply report whether a seal can or cannot be defeated in a specified period of time.

With the goal of trying to better classify defeats, we at LANL have developed what we call the LANL Seal Defeat Categorization Scheme. This classification scheme has proven to be useful in presenting seal vulnerabilities to seal developers, manufacturers, and users. It is not, however, the only possible approach.

Under the LANL scheme, we classify successful attacks into four categories: type 1, 2a, 2b, or 3. In a type 1 defeat, tampering is not detected if the "usual" seal inspection process is followed. See figure 1. The usual process is that routinely or typically employed by the end-user. For most seals, this is the protocol recommended by the developer or manufacturer of the seal. A type 1 defeat, however, will be detected if unusual efforts are taken. For many seals, an example of an unusual inspection protocol would be to disassemble the seal and examined it in great detail to look for tampering.

In a type 2a defeat, tampering is not detected if the usual inspection protocol is followed and if the user visually studies the exterior of the seal (plus any internal parts that can be seen without opening the seal) to look for evidence of entry. See figure 2a. The visual inspection can be done with either the naked eye or a hand-held magnifier.

In a type 2b defeat, tampering is not detected if the usual inspection protocol is followed and if the user disassembles the seal and meticulously examines the interior and the exterior of the seal visually (with the naked eye or a hand-held magnifier) to look for evidence of entry. See figure 2b. In a type 3 defeat, tampering cannot be detected, even if the most advanced postmortem analysis is undertaken. See figure 3. State-of-the-art techniques in forensics, material science, or microscopy will not be able to tell that the seal has been defeated.

Classifying a defeat as type 3 is problematic in that it is difficult to be absolutely certain that no technology anywhere in the world has the ability to detect the tampering. Despite this problem, we believe we have demonstrated a number of type 3 defeats at LANL [13].

If a non-type 3 defeat is successful in a seal application where the "usual" inspection protocol automatically includes meticulous visual examination of the exterior or interior of the seal, the defeat is classified as 2a or 2b, respectively, rather than as a type 1 defeat.

Concluding Remarks

Seal vulnerability assessment, by its very nature, is difficult to quantify, specify, and standardize. Unlike locks and safes, for example, defeating a seal involves more than just breaking in with force or manipulation; the critical issue is whether the seal user can be fooled in the process. For some applications, it is sufficient for an adversary merely to fool the seal user for a limited period of time. If the attack is eventually discovered, it may not matter.

There are other complicating issues as well. Unlike materials testing, vulnerability assessments will usually yield different results when performed by different personnel at different times. A devastating defeat identified by one team of assessors may be totally missed by another.

Vulnerability assessments are also intrinsically open-ended. There is no way to know when a particular vulnerability assessment has found all the vulnerabilities, or even the most important ones. Assessments are usually

undertaken as short duration projects with fixed budgets and completion times. Adversaries may not be constrained this way.

Given the complexity of seal defeat issues, it seems unlikely that any generic standard or set of guidelines will ever be totally satisfactory in specifying seal vulnerability assessment. The purpose of this paper was to attempt to identify attributes of effective vulnerability assessments.

Perhaps these or similar attributes can be incorporated at least partially into future standards and assessments. These attributes include: a clear understanding of what seal vulnerability assessment is and why it is undertaken; use of appropriate assessment personnel; assessment at the earliest possible stage of seal development; analysis conducted with the proper emphasis and context; rejection of findings of zero vulnerabilities; avoidance of the term "tamper-proof"; attempts to classify the severity or thoroughness of the defeats; and complete reporting of the vulnerability assessment findings.

Acknowledgements

This work was performed under the auspices of the United States Department of Energy. Anthony Garcia provided useful input.

References

[1] Kissane, C.P. and DeSanto, J., "Cargo Theft Loss Prevention Techniques," in Handbook of Loss Prevention and Crime Prevention, Fennelly, L.J., Editor, Butterworth, Boston, 1992, pp. 689-691.

[2] Department of Transportation Physical Security Manual, GPO Report # 982-2-5, November 29, 1977.

[3] Staehle, G. (Editor), DOE's Tags and Seals Program, Verification Technologies, U.S. Department of Energy Report DOE/DP/OAC/VT-92B, October, 1992, pp. 4-41.

[4] Anon., "Advances in Treaty Verification Technology," Energy and Technology Review, January 1992, pp. 4-60.

[5] "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material," Draft Regulatory Guide DG-5005, U.S. Nuclear Regulatory Commission, January 1996, pp. 1-13.

[6] Horton, P.R.V. and Waddoups, I.G., "Tamper-Indicating Devices and Safeguards Seals Evaluation Test Report," Sandia National Laboratories Report SAND93-1726/2, August 1995.

[7] Rosette J.L., Improving Tamper-Evident Packaging. Lancaster, PA: Technomic Publishing, 1992, pp. 1-34.

[8] "Standard Guide for Inspection and Evaluation of Tampering of Security Seals," ASTM Standard F1158-88, ASTM, August 1988, p. 691.

[9] "Standard Practice for Classifying the Relative Performance of the Physical Properties of Security Seals," ASTM Standard F1157-90, ASTM, March 1990, pp. 686-690.

[10] "Federal Specification for Seals, Antipilferage," U.S. Government Specification FF-S-2738, Superintendent of Documents, Washington, D.C., June 7, 1990, pp. 1-19.

[11] "Specifications for Security seals," British Standard BS 7480:1992, British Standards Board, February 28, 1992, pp. 1-14.

[12] Johnston, R.G., "Vulnerability Assessment of 40 Commercial and Government Tags and Seals," Proceedings of the Security Seal and Tamper-Indicating Device Forum, Naval Facilities Engineering Service Center, Oxnard California, August 23-24, 1995, pp. 2-1 to 2-7.

[13] Johnston, R.G., Garcia, A.R.E., and Grace, W. Kevin, “Vulnerability Assessment of Passive Tamper-Indicating Seal,” Journal of Nuclear Materials Management, INMM, Vol. 224, July 1995, pp. 24-29.

[14] Johnston, R.G., "Vulnerability Assessment of Tamper-Indicating Seals," Proceedings of the ASIS/DoD Security Seal Symposium, Naval Facilities Engineering Service Center, Santa Barbara, CA, February 6-7, 1996, (in press).

FIG. 1 - Type 1 defeat. A seal attack is classified as a type 1 defeat if it goes undetected when the user employs the usual, standard, or recommended protocol for inspecting the seal. For many seals, this protocol does not involve extremely careful visual examination of the seal, nor high-technology methods of examination.

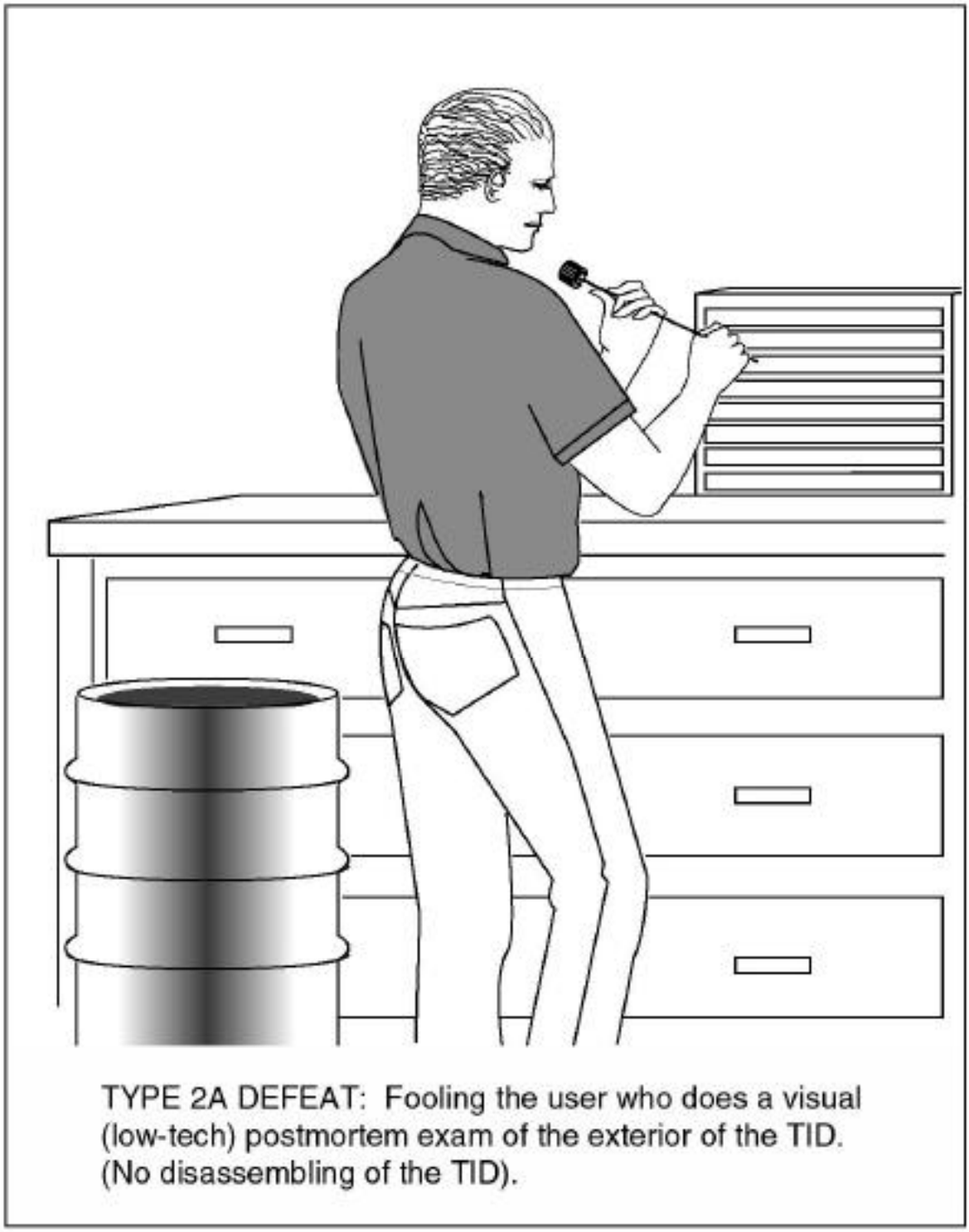

FIG. 2a - Type 2a defeat. A seal attack is classified as a type 2a defeat if it goes undetected when the user employs the usual, standard, or recommended protocol for inspecting the seal, and even when the user spends considerable effort in visually examining the exterior of the seal, or any internal parts visible from outside the seal.

FIG. 2b - Type 2b defeat. A seal attack is classified as a type 2b defeat if it goes undetected when the user employs the usual, standard, or recommended protocol for inspecting the seal, and even when the user disassembles the seal and spends considerable effort in visually examining the interior and exterior of the seal.

FIG. 3 - Type 3 defeat. A seal attack is classified as a type 3 defeat if it goes undetected regardless of the length of time devoted to inspection, and regardless of the inspection technique or high technology used.